Primitive and totally primitive Fricke families with applications

Ho Yun Jung, Ja Kyung Koo and Dong Hwa Shin

Abstract

We introduce the primitivity of Fricke families, and give some examples. As its application, we first construct generators of the function field of the modular curve of level N in terms of Fricke functions and Siegel functions, respectively. Furthermore, we use the special values of a certain function in a totally primitive Fricke family of level N in order to generate ray class fields of imaginary quadratic fields.

1 Introduction

For a positive integer N, let $\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv I_2 \pmod N\}$ be the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level N. This group acts on the complex upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ and $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\mathrm{i}\infty\}$ as fractional linear transformations. One can then give the orbit space $X(N) = \Gamma(N)\backslash\mathbb{H}^*$ the structure of a compact Riemann surface, called the *modular curve* of level N ([12, §1.5]). Let $\mathbb{C}(X(N))$ be the field of meromorphic functions on $X(N)$ which is a Galois extension of $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ with

$$\mathrm{Gal}\,(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \simeq \mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\},$$

where $j(\tau)$ is the elliptic modular function ([10, Theorem 2 in Chapter 6]). Furthermore, we denote by $\mathcal{F}_N$ the subfield of $\mathbb{C}(X(N))$ consisting of functions whose Fourier coefficients lie in the Nth cyclotomic field $\mathbb{Q}(\zeta_N)$, where $\zeta_N = e^{2\pi\mathrm{i}/N}$. Then, $\mathcal{F}_N$ is also a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$ whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ (see §2).

For $N \geq 2$, let

$$\mathcal{V}_N = \{\mathbf{v} \in \mathbb{Q}^2 \mid N \text{ is the least positive integer so that } N\mathbf{v} \in \mathbb{Z}^2\}.$$

We call a family $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ of functions in $\mathcal{F}_N$ a *Fricke family* of level N if it satisfies the following three conditions:

2010 *Mathematics Subject Classification*. Primary 11F03, Secondary 11G16.

Key words and phrases. Fricke families, modular functions, modular units.

The first named author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A5A1008055). The third named (corresponding) author was supported by Hankuk University of Foreign Studies Research Fund of 2016.

(F1) Every $h_{\mathbf{v}}(\tau)$ is holomorphic on $\mathbb{H}$.

(F2) $h_{\mathbf{u}}(\tau) = h_{\mathbf{v}}(\tau)$ if $\mathbf{u} \equiv \pm\mathbf{v} \pmod{\mathbb{Z}^2}$.

(F3) $h_{\mathbf{v}}(\tau)^{\alpha} = h_{\alpha^T\mathbf{v}}(\tau)$ for $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$, where α^T stands for the transpose of α.

As for a Fricke family, Kubert and Lang first gave its definition without the condition (F1) ([4, pp. 32–33]). Recently, Eum and Shin ([3]) classified all Fricke families of level N when $N \equiv 0 \pmod 4$. See also [9].

We say that a Fricke family $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ of level N is *primitive* if the condition (F2) is strengthened in such a way that

$$h_{\mathbf{u}}(\tau) = h_{\mathbf{v}}(\tau) \iff \mathbf{u} \equiv \pm\mathbf{v} \pmod{\mathbb{Z}^2}.$$

Moreover, we say that $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is *totally primitive* if $\{h_{\mathbf{v}}(\tau)^n\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive for every positive integer n. In this paper, we shall present several examples of Fricke families which are primitive or totally primitive (Examples 3.1, 3.2 and 3.3).

As is well known, we have

$$\mathbb{C}(X(N)) = \mathbb{C}\left(j(\tau),\, f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau),\, f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)\right),$$

where $f_{\mathbf{v}}(\tau)$ ($\mathbf{v} \in \mathcal{V}_N$) are the classical Fricke functions (see §2 and [2, Proposition 7.5.1]). Since the modular curve $X(N)$ is an algebraic curve, its function field $\mathbb{C}(X(N))$ can be generated by two functions ([11, Theorem 1.9 and Proposition 1.17 in Chapter VI]). As an application of primitive Fricke families, we shall first construct a primitive generator of $\mathbb{C}(X(N))$ over the field $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ in terms of Fricke functions $f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)$ and $f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)$ (Theorem 4.3) which belong to a primitive Fricke family. We shall further present a primitive generator of $\mathbb{C}(X(N))$ over $\mathbb{C}(X(1))$ by making use of only Siegel functions as members of a totally primitive Fricke family (Theorem 4.4 and Remark 4.5).

Let K be an imaginary quadratic field of discriminant d_K, and let $\mathcal{O}_K$ be its ring of integers. If we set

$$\tau_K = (d_K + \sqrt{d_K})/2,$$

then we see that $\tau_K \in \mathbb{H}$ and $\mathcal{O}_K = \mathbb{Z}\tau_K + \mathbb{Z}$ ([1, §5.B]). By H_K we mean the Hilbert class field of K, and by $K_{(N)}$ the ray class field modulo $N\mathcal{O}_K$. Let $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ be a totally primitive Fricke family of level N. For all but finitely many K, we shall show that if the special value $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)$ is nonzero, then $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n$ generates $K_{(N)}$ over H_K for any nonzero integer n (Theorem 5.2 and Remark 5.3).

Based on this work, Koo et al. established the concept of a (totally) primitive Siegel family consisting of meromorphic Siegel modular functions of higher genus g (≥ 2) ([7, Definition 3.1]). They further constructed explicit generators of the field of Siegel modular functions of level N ($\neq 2,\, 2^g - 1,\, 2(2^g - 1)$) over the field of Siegel modular functions of level 1 ([7, Proposition 3.3 and Theorem 6.2]). To this end, they reduced each theta constant of genus g to a product of Siegel functions of one-variable, and then made use of the idea of Example 3.1. We also notice that there is a recent attempt ([5]) to get a higher genus version of Theorem 5.2 for CM-fields.

2 Meromorphic modular functions

Let N be a positive integer. The group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ ($\simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$) acts on the field $\mathcal{F}_N$ as follows ([10, Theorem 3 in Chapter 6]): One can decompose $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ uniquely as

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \text{ with } G_N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Let $h(\tau)$ be an element of $\mathcal{F}_N$ whose Fourier expansion with respect to $q^{1/N} = e^{2\pi \mathrm{i}\tau/N}$ is given by

$$h(\tau) = \sum_{n \gg -\infty} c_n q^{n/N} \quad (c_n \in \mathbb{Q}(\zeta_N)).$$

(A1) $\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \in G_N$ acts on $h(\tau)$ as

$$h(\tau)^{\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]} = \sum_{n \gg -\infty} c_n^{\sigma_d} q^{n/N},$$

where σ_d is the automorphism of the cyclotomic field $\mathbb{Q}(\zeta_N)$ determined by $\zeta_N^{\sigma_d} = \zeta_N^d$.

(A2) $\alpha \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ acts on $h(\tau)$ by

$$h(\tau)^\alpha = (h \circ \widetilde{\alpha})(\tau),$$

where $\widetilde{\alpha}$ is any inverse image of α under the reduction $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$.

For a lattice Λ in $\mathbb{C}$, let

$$g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}, \quad g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6} \quad \text{and} \quad \Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2.$$

The *Weierstrass $\wp$-function* relative to Λ is defined by

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left\{ \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right\} \quad (z \in \mathbb{C})$$

with a double pole at each lattice point, and no other poles ([10, p. 8]). By the *Weierstrass σ-function* relative to Λ we mean the infinite product

$$\sigma(z; \Lambda) = z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) e^{z/\lambda + (1/2)(z/\lambda)^2} \quad (z \in \mathbb{C}).$$

Taking logarithmic derivative, we derive the *Weierstrass ζ-function*

$$\zeta(z; \Lambda) = \frac{\sigma'(z; \Lambda)}{\sigma(z; \Lambda)} = \frac{1}{z} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{z-\lambda} + \frac{1}{\lambda} + \frac{z}{\lambda^2} \right) \quad (z \in \mathbb{C}).$$

Since $\zeta'(z;\,\Lambda) = -\wp(z;\,\Lambda)$ which is periodic with respect to Λ, for each $\lambda \in \Lambda$ we obtain a constant $\eta(\lambda;\,\Lambda)$ satisfying

$$\zeta(z+\lambda;\,\Lambda) - \zeta(z;\,\Lambda) = \eta(\lambda;\,\Lambda) \quad (z \in \mathbb{C}).$$

Now, let $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. We define the *Fricke function* $f_{\mathbf{v}}(\tau)$ by

$$f_{\mathbf{v}}(\tau) = -2^7 3^5 \frac{g_2(\tau) g_3(\tau)}{\Delta(\tau)} \wp_{\mathbf{v}}(\tau) \quad (\tau \in \mathbb{H}), \tag{1}$$

where $g_2(\tau) = g_2([\tau,\,1])$, $g_3(\tau) = g_3([\tau,\,1])$, $\Delta(\tau) = \Delta([\tau,\,1])$ and $\wp_{\mathbf{v}}(\tau) = \wp(v_1\tau + v_2;\,[\tau, 1])$. Note that $g_2(\tau)$, $g_3(\tau)$ and $\Delta(\tau)$ are holomorphic on $\mathbb{H}$, and $\Delta(\tau)$ has no zeros on $\mathbb{H}$ ([10, Theorem 3 in Chapter 3]). We also define the *Siegel function* $g_{\mathbf{v}}(\tau)$ by

$$g_{\mathbf{v}}(\tau) = e^{-(v_1\eta(\tau;\,[\tau,1]) + v_2\eta(1;\,[\tau,1]))(v_1\tau+v_2)/2} \sigma(v_1\tau + v_2;\,[\tau,\,1])\eta(\tau)^2 \quad (\tau \in \mathbb{H}), \tag{2}$$

where

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q^{1/24} \prod_{n=1}^{\infty}(1-q^n) \quad (\tau \in \mathbb{H})$$

is the *Dedekind η-function*. As is well known, if $N \geq 2$, then $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ and $\{g_{\mathbf{v}}(\tau)^{12N}\}_{\mathbf{v}\in\mathcal{V}_N}$ are Fricke families of level N ([10, §6.2 and 6.3] and [4, Proposition 1.3 in Chapter 2]). Moreover, $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive ([1, Lemma 10.4] and the definition (1)).

For $x \in \mathbb{R}$, let $\langle x \rangle$ be the fractional part of x in the interval $[0, 1)$, and set

$$\langle \pm x \rangle = \min(\langle x \rangle, \langle -x \rangle).$$

Furthermore, let $\mathbf{B}_2(x) = x^2 - x + 1/6$ be the second Bernoulli polynomial.

Lemma 2.1. *Let $N \geq 2$.*

(i) *If* $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$, *then we have* $\mathrm{ord}_q\ g_{\mathbf{v}}(\tau) = (1/2)\mathbf{B}_2(\langle v_1 \rangle)$.

(ii) *Let* $\mathbf{u}$, $\mathbf{v}$, $\mathbf{u}'$, $\mathbf{v}' \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$ *such that* $\mathbf{u} \not\equiv \pm\mathbf{v} \pmod{\mathbb{Z}^2}$ *and* $\mathbf{u}' \not\equiv \pm\mathbf{v}' \pmod{\mathbb{Z}^2}$. *Then, the function*

$$\frac{f_{\mathbf{u}}(\tau) - f_{\mathbf{v}}(\tau)}{f_{\mathbf{u}'}(\tau) - f_{\mathbf{v}'}(\tau)} = \frac{\wp_{\mathbf{u}}(\tau) - \wp_{\mathbf{v}}(\tau)}{\wp_{\mathbf{u}'}(\tau) - \wp_{\mathbf{v}'}(\tau)}$$

in $\mathcal{F}_N$ has neither zeros nor poles on $\mathbb{H}$.

(iii) *If* $\mathbf{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$, $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathcal{V}_N$ *such that* $\mathbf{u}+\mathbf{v}$, $\mathbf{u}-\mathbf{v} \in \mathcal{V}_N$, *then*

$$\mathrm{ord}_q\ (\wp_{\mathbf{u}}(\tau) - \wp_{\mathbf{v}}(\tau)) = \min(\langle \pm u_1 \rangle,\, \langle \pm v_1 \rangle).$$

Proof. (i) See [4, p. 39].

(ii) See [4, Theorem 6.1 in Chapter 2].

(iii) See [4, Lemma 6.2 in Chapter 2].

□

3 Examples of primitive and totally primitive Fricke families

Let $N \geq 2$. In this section, we shall give several examples of primitive and totally primitive Fricke families.

EXAMPLE 3.1. Consider the Fricke family $\{g_{\mathbf{v}}(\tau)^{12N}\}_{\mathbf{v}\in\mathcal{V}_N}$ consisting of $12N$th powers of Siegel functions. We want to show that the family is totally primitive.

Suppose that

$$g_{\mathbf{u}}(\tau)^{12Nn} = g_{\mathbf{v}}(\tau)^{12Nn} \quad \text{for some } \mathbf{u}, \mathbf{v} \in \mathcal{V}_N \text{ and } n \in \mathbb{N}.$$

Since there is an element α of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ such that

$$\alpha^T \mathbf{u} \equiv \pm \begin{bmatrix} 1/N \\ 0 \end{bmatrix} \pmod{\mathbb{Z}^2},$$

we may assume by (F3) that

$$g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12Nn} = g_{\mathbf{v}}(\tau)^{12Nn} \text{ for } \mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathcal{V}_N. \tag{3}$$

Applying $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ to both sides of (3), we attain that

$$g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12Nn} = g_{\left[\begin{smallmatrix} -v_2 \\ v_1 \end{smallmatrix}\right]}(\tau)^{12Nn}. \tag{4}$$

By Lemma 2.1 (i), we obtain from (3) and (4) that

$$6Nn\mathbf{B}_2(1/N) = 6Nn\mathbf{B}_2(\langle v_1 \rangle) \quad \text{and} \quad 6Nn\mathbf{B}_2(0) = 6Nn\mathbf{B}_2(\langle -v_2 \rangle),$$

respectively. Thus we deduce by considering the graph of $y = \mathbf{B}_2(x)$ that

$$v_1 \equiv \pm 1/N \pmod{\mathbb{Z}} \quad \text{and} \quad v_2 \equiv 0 \pmod{\mathbb{Z}},$$

and hence $\mathbf{v} \equiv \pm \begin{bmatrix} 1/N \\ 0 \end{bmatrix} \pmod{\mathbb{Z}^2}$. This observation implies that the Fricke family $\{g_{\mathbf{v}}(\tau)^{12N}\}_{\mathbf{v}\in\mathcal{V}_N}$ is totally primitive.

EXAMPLE 3.2. Assume that N is odd and the set

$$Q_N = [1, N/2] \cap \{a \in \mathbb{Z} \mid a \not\equiv \pm 1 \pmod{N} \text{ and } a^2 \equiv \pm 1 \pmod{N}\}.$$

is nonempty. Let $a \in Q_N$. If we set

$$h_{\mathbf{v}}(\tau) = f_{\mathbf{v}}(\tau) - f_{a\mathbf{v}}(\tau) \quad (\mathbf{v} \in \mathcal{V}_N), \tag{5}$$

then we get a Fricke family $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ of level N. We want to show that $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive, but not totally primitive.

Suppose that

$$h_{\mathbf{a}}(\tau) = h_{\mathbf{b}}(\tau) \quad \text{for some } \mathbf{a},\, \mathbf{b} \in \mathcal{V}_N.$$

By applying an action of the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$, if necessary, we may assume by (F3) that

$$h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) = h_{\mathbf{b}}(\tau) \quad \text{with } \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}. \tag{6}$$

The action of $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ on both sides of (6) yields

$$h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau) = h_{\left[\begin{smallmatrix}-b_2\\b_1\end{smallmatrix}\right]}(\tau). \tag{7}$$

By the definitions (1) and (5), we obtain from (6) and (7) that

$$\begin{aligned} \wp_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau) &= \wp_{\left[\begin{smallmatrix}b_1\\b_2\end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix}ab_1\\ab_2\end{smallmatrix}\right]}(\tau), \\ \wp_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix}0\\a/N\end{smallmatrix}\right]}(\tau) &= \wp_{\left[\begin{smallmatrix}-b_2\\b_1\end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix}-ab_2\\ab_1\end{smallmatrix}\right]}(\tau). \end{aligned}$$

Comparing the q-orders by making use of Lemma 2.1 (iii), we get

$$1/N = \min(\langle \pm b_1 \rangle,\, \langle \pm a b_1 \rangle) \quad \text{and} \quad 0 = \min(\langle \pm b_2 \rangle,\, \langle \pm a b_2 \rangle),$$

respectively. We then deduce from the fact $a^2 \equiv \pm 1 \pmod N$ that

$$b_1 \equiv \pm 1/N \text{ or } \pm\, a/N \pmod{\mathbb{Z}} \quad \text{and} \quad b_2 \equiv 0 \pmod{\mathbb{Z}}.$$

If $b_1 \equiv \pm a/N \pmod{\mathbb{Z}}$, then we see that

$$\begin{aligned} f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau) &= h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) \quad \text{by the definition (5)} \\ &= h_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau) \quad \text{by (6) and (F2)} \\ &= f_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}a^2/N\\0\end{smallmatrix}\right]}(\tau) \quad \text{by the definition (5)} \\ &= f_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) \quad \text{by the fact } a^2 \equiv \pm 1 \pmod N \text{ and (F2)}, \end{aligned}$$

from which it follows that $f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau)$. But, this is impossible because $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive and $a \not\equiv \pm 1 \pmod N$. Thus we attain $\mathbf{b} \equiv \pm \begin{bmatrix} 1/N \\ 0 \end{bmatrix} \pmod{\mathbb{Z}^2}$, which shows that $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive.

On the other hand, we derive by the definition (5), the fact $a^2 \equiv \pm 1 \pmod N$ and (F2) that

$$h_{a\mathbf{v}}(\tau) = f_{a\mathbf{v}}(\tau) - f_{a^2\mathbf{v}}(\tau) = f_{a\mathbf{v}}(\tau) - f_{\mathbf{v}}(\tau) = -h_{\mathbf{v}}(\tau) \quad (\mathbf{v} \in \mathcal{V}_N),$$

which gives rise to $h_{a\mathbf{v}}(\tau)^2 = h_{\mathbf{v}}(\tau)^2$. Here we note that $a\mathbf{v} \not\equiv \pm\mathbf{v} \pmod{\mathbb{Z}^2}$ due to the fact $a \not\equiv \pm 1 \pmod N$. Hence $\{h_{\mathbf{v}}(\tau)^2\}_{\mathbf{v}\in\mathcal{V}_N}$ is not primitive.

Therefore, the Fricke family $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive, whereas not totally primitive.

EXAMPLE 3.3. Let $N \geq 7$ and $\gcd(6, N) = 1$. We claim that the Fricke family $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is totally primitive.

Suppose on the contrary that it is not totally primitive. Then we have

$$f_{\mathbf{a}}(\tau)^n = f_{\mathbf{b}}(\tau)^n$$

for some integer $n \geq 2$ and $\mathbf{a}, \mathbf{b} \in \mathcal{V}_N$ such that $\mathbf{a} \not\equiv \pm\mathbf{b} \pmod{\mathbb{Z}^2}$. By applying an action of the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$, if necessary, we may assume that

$$f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) = \zeta f_{\left[\begin{smallmatrix}b_1\\b_2\end{smallmatrix}\right]}(\tau) \tag{8}$$

for some nth root of unity ζ and $\begin{bmatrix}b_1\\b_2\end{bmatrix} \in \mathcal{V}_N$ such that

$$\begin{bmatrix}b_1\\b_2\end{bmatrix} \not\equiv \pm\begin{bmatrix}1/N\\0\end{bmatrix} \pmod{\mathbb{Z}^2}. \tag{9}$$

Through the action of $\begin{bmatrix}1&0\\1&1\end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ on both sides of (8), we get by (F3) and (A2) that

$$f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) = \zeta f_{\left[\begin{smallmatrix}b_1+b_2\\b_2\end{smallmatrix}\right]}(\tau). \tag{10}$$

We see from (8) and (10) that

$$f_{\left[\begin{smallmatrix}b_1\\b_2\end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix}b_1+b_2\\b_2\end{smallmatrix}\right]}(\tau).$$

Since $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive, we attain that

$$\begin{bmatrix}b_1\\b_2\end{bmatrix} \equiv \pm\begin{bmatrix}b_1+b_2\\b_2\end{bmatrix} \pmod{\mathbb{Z}^2}.$$

If $\begin{bmatrix}b_1\\b_2\end{bmatrix} \equiv -\begin{bmatrix}b_1+b_2\\b_2\end{bmatrix} \pmod{\mathbb{Z}^2}$, then we get $2b_1 \equiv -b_2 \pmod{\mathbb{Z}}$ and $2b_2 \equiv 0 \pmod{\mathbb{Z}}$, and so $4\begin{bmatrix}b_1\\b_2\end{bmatrix} \equiv \begin{bmatrix}0\\0\end{bmatrix} \pmod{\mathbb{Z}^2}$. But, this is impossible because $\begin{bmatrix}b_1\\b_2\end{bmatrix} \in \mathcal{V}_N$ and $N \neq 4$. Thus we must have

$$\begin{bmatrix}b_1\\b_2\end{bmatrix} \equiv \begin{bmatrix}b_1+b_2\\b_2\end{bmatrix} \pmod{\mathbb{Z}^2},$$

and hence $b_2 \equiv 0 \pmod{\mathbb{Z}}$. Write $b_1 = a/N$ for an integer a which is relatively prime to N and $a \not\equiv \pm 1 \pmod{N}$ by (9). By applying (F2) to the function $f_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau)$, we may further assume that $1 < a \leq N/2$. We then find by (8) that

$$\zeta = \frac{f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)}{f_{\left[\begin{smallmatrix}a/N\\0\end{smallmatrix}\right]}(\tau)},$$

and hence we obtain by acting $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in G_N$ that

$$\zeta^{-1} = \frac{f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)}{f_{\left[\begin{smallmatrix} a/N \\ 0 \end{smallmatrix}\right]}(\tau)}$$

due to (A1) and (F3). Since $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive and $a \not\equiv \pm 1 \pmod N$, we conclude $\zeta = -1$, and so

$$f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) = -f_{\left[\begin{smallmatrix} a/N \\ 0 \end{smallmatrix}\right]}(\tau). \tag{11}$$

The action of $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ on both sides of (11) yields

$$f_{\left[\begin{smallmatrix} a/N \\ 0 \end{smallmatrix}\right]}(\tau) = -f_{\left[\begin{smallmatrix} a^2/N \\ 0 \end{smallmatrix}\right]}(\tau) \tag{12}$$

by (F3). It then follows from (11) and (12) that

$$f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix} a^2/N \\ 0 \end{smallmatrix}\right]}(\tau),$$

which implies that

$$a^2 \equiv \pm 1 \pmod N \tag{13}$$

because $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive. Acting $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in G_N$ on both sides of (11), we also obtain by (F3) that

$$f_{\left[\begin{smallmatrix} 2/N \\ 0 \end{smallmatrix}\right]}(\tau) = -f_{\left[\begin{smallmatrix} 2a/N \\ 0 \end{smallmatrix}\right]}(\tau). \tag{14}$$

We then derive by the definition (1), (11) and (14) that

$$\wp_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix} 2/N \\ 0 \end{smallmatrix}\right]}(\tau) = -\wp_{\left[\begin{smallmatrix} a/N \\ 0 \end{smallmatrix}\right]}(\tau) + \wp_{\left[\begin{smallmatrix} 2a/N \\ 0 \end{smallmatrix}\right]}(\tau).$$

By Lemma 2.1 (iii) and the fact $1 \le a \le N/2$, we achieve that

$$\begin{aligned}
\mathrm{ord}_q\left(\wp_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - \wp_{\left[\begin{smallmatrix} 2/N \\ 0 \end{smallmatrix}\right]}(\tau)\right) &= \min(\langle \pm 1/N\rangle, \langle \pm 2/N\rangle) \\
&= 1/N \\
&= \mathrm{ord}_q\left(-\wp_{\left[\begin{smallmatrix} a/N \\ 0 \end{smallmatrix}\right]}(\tau) + \wp_{\left[\begin{smallmatrix} 2a/N \\ 0 \end{smallmatrix}\right]}(\tau)\right) \\
&= \min(\langle \pm a/N\rangle, \langle \pm 2a/N\rangle) \\
&= \min(\min(a/N,\, (N-a)/N),\, \min(2a/N,\, (N-2a)/N)) \\
&= \begin{cases} a/N & \text{if } 1 \le a \le N/3, \\ (N-2a)/N & \text{if } N/3 < a \le N/2. \end{cases}
\end{aligned}$$

Moreover, since $a \neq 1$, we must get $1/N = (N-2a)/N$, and so $a = (N-1)/2$. We then obtain from (13) that

$$(N^2 - 2N + 1)/4 \equiv \pm 1 \pmod N.$$

But, this contradicts the assumption $N \ge 7$.

Therefore, we conclude that the primitive Fricke family $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is also totally primitive.

4 Generators of function fields

Let $N \geq 2$. As an application of (totally) primitive Fricke families, we shall construct primitive generators of $\mathbb{C}(X(N))$ and $\mathcal{F}_N$ over $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ and $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$, respectively.

PROPOSITION 4.1. *Let $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ be a primitive Fricke family of level N. Then we have*

$$\mathbb{C}(X(N)) = \mathbb{C}\left(j(\tau), h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau),\, h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)\right).$$

PROOF. Recall that $\mathbb{C}(X(N))$ is a Galois extension of $\mathbb{C}(X(1))$ with

$$\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \simeq \mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N).$$

Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $\mathrm{SL}_2(\mathbb{Z})$ which leaves both $h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)$ and $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)$ fixed. We then see by (F3) that

$$h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) = h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{\gamma} = h_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\tau) \quad \text{and} \quad h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau) = h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{\gamma} = h_{\left[\begin{smallmatrix}c/N\\d/N\end{smallmatrix}\right]}(\tau).$$

Now that $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive, we get

$$\begin{bmatrix} a/N \\ b/N \end{bmatrix} \equiv \pm \begin{bmatrix} 1/N \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} c/N \\ d/N \end{bmatrix} \equiv \pm \begin{bmatrix} 0 \\ 1/N \end{bmatrix} \pmod{\mathbb{Z}^2}.$$

Moreover, we deduce from $\det(\gamma) = ad - bc = 1$ that $a \equiv d \equiv \pm 1$; and hence $\gamma \equiv \pm I_2 \pmod{N}$ and so $\gamma \in \pm\Gamma(N)$.

This yields by Galois theory that $h_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)$ and $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)$ generate $\mathbb{C}(X(N))$ over $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$. □

EXAMPLE 4.2. Since $\{g_{\mathbf{v}}(\tau)^{12N}\}_{\mathbf{v}\in\mathcal{V}_N}$ is totally primitive by Example 3.1, $\{g_{\mathbf{v}}(\tau)^{12Nn}\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive for each positive integer n. By applying Proposition 4.1 to each family $\{g_{\mathbf{v}}(\tau)^{12Nn}\}_{\mathbf{v}\in\mathcal{V}_N}$ and using the fact that $\mathbb{C}(X(N))$ is a field, we obtain

$$\mathbb{C}(X(N)) = \mathbb{C}\left(j(\tau),\, g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{12Nn},\, g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{12Nn}\right)$$

for any nonzero integer n.

THEOREM 4.3. *We have*

(i) $\mathbb{C}(X(N)) = \mathbb{C}\left(j(\tau),\, f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1}\right)$.

(ii) $\mathcal{F}_N = \mathbb{Q}\left(j(\tau),\, \zeta_N\left(f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1}\right)\right)$.

PROOF. (i) Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $\mathrm{SL}_2(\mathbb{Z})$ which leaves $f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-1}$ fixed. By (F3) we attain that

$$f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-1} = (f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-1})^{\gamma} = f_{\left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau)^{-1},$$

from which it follows that

$$f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-1} - f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau)^{-1} = \frac{f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)}{f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau)}. \quad (15)$$

If $\begin{bmatrix} a/N \\ c/N \end{bmatrix} \not\equiv \pm \begin{bmatrix} 1/N \\ 0 \end{bmatrix} \pmod{\mathbb{Z}^2}$, then we deduce

$$f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right]}(\tau) \neq 0$$

due to the fact that $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v} \in \mathcal{V}_N}$ is primitive. We then see from (15) that

$$f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) \neq 0,$$

which yields $\begin{bmatrix} c/N \\ d/N \end{bmatrix} \not\equiv \pm \begin{bmatrix} 0 \\ 1/N \end{bmatrix} \pmod{\mathbb{Z}^2}$. Now, consider the relation

$$f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau) f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau) = \frac{f_{\left[\begin{smallmatrix} c/N \\ d/N \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)}{f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} a/N \\ b/N \end{smallmatrix}\right]}(\tau)} \quad (16)$$

derived from (15). Since $g_2(\zeta_3) = 0$ ([10, p. 37]), the left side of (16) vanishes at ζ_3 by the definition (1), whereas the right side of (16) has neither zeros nor poles on $\mathbb{H}$ by Lemma 2.1 (ii). This gives a contradiction. Thus we achieve that

$$\begin{bmatrix} a/N \\ b/N \end{bmatrix} \equiv \pm \begin{bmatrix} 1/N \\ 0 \end{bmatrix} \pmod{\mathbb{Z}^2},$$

and get by (15) that

$$\begin{bmatrix} c/N \\ d/N \end{bmatrix} \equiv \pm \begin{bmatrix} 0 \\ 1/N \end{bmatrix} \pmod{\mathbb{Z}^2}.$$

Furthermore, we obtain by the fact $\det(\gamma) = ad - bc = 1$ that $a \equiv d \equiv \pm 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$; and hence $\gamma \in \pm\Gamma(N)$. This proves (i) by Galois theory.

(ii) We get by (i) and [12, Theorem 6.6] that

$$\mathcal{F}_N = \mathbb{Q}\left(\zeta_N,\, j(\tau),\, f_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{-1}\right).$$

Thus, if we set

$$F = \mathbb{Q}\left(j(\tau),\, \zeta_N\left(f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1}\right)\right),$$

then $\mathrm{Gal}(\mathcal{F}_N/F)$ is a subgroup of

$$G_N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Let $\gamma = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ be an element of G_N which fixes the field F elementwise. We then see by (F3) and (A1) that

$$\begin{aligned} \zeta_N\left(f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1}\right) &= \left(\zeta_N\left(f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1}\right)\right)^{\gamma} \\ &= \zeta_N^d\left(f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\d/N\end{smallmatrix}\right]}(\tau)^{-1}\right), \end{aligned}$$

from which it follows that

$$\zeta_N^{d-1} = \frac{f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1}}{f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) - f_{\left[\begin{smallmatrix}0\\d/N\end{smallmatrix}\right]}(\tau)^{-1}}. \tag{17}$$

Here, we note by (F2) and (F3) that the right side of (17) is fixed by the action of $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Thus we attain by (A1) that

$$\zeta_N^{d-1} = (\zeta_N^{d-1})^{\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]} = \zeta_N^{-(d-1)},$$

and so $\zeta_N^{d-1} = \pm 1$. If $\zeta_N^{d-1} = -1$, then we derive by (17) that

$$2f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau) = f_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{-1} + f_{\left[\begin{smallmatrix}0\\d/N\end{smallmatrix}\right]}(\tau)^{-1}. \tag{18}$$

Due to (F3), the right side of (18) is fixed by the action of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, but we see that

$$2f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]} = 2f_{\left[\begin{smallmatrix}1/N\\1/N\end{smallmatrix}\right]}(\tau) \neq 2f_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)$$

because $\{f_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ is primitive. This yields a contradiction. Therefore, we must have $\zeta_N^{d-1} = 1$; and hence $d \equiv 1 \pmod{N}$ and $\gamma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. This implies by Galois theory that $F = \mathcal{F}_N$, as desired.

□

By using the idea of Example 3.1, we further establish the following theorem.

THEOREM 4.4. *Let n be any nonzero integer.*

(i) $\mathbb{C}(X(N)) = \mathbb{C}\left(j(\tau),\, g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{24Nn}\right)$.

(ii) $\mathcal{F}_N = \mathbb{Q}\left(j(\tau),\, \zeta_N g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{24Nn}\right)$.

PROOF. (i) Let

$$g(\tau) = g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{24Nn},$$

which belongs to $\mathbb{C}(X(N))$. And, let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $\mathrm{SL}_2(\mathbb{Z})$ leaving $g(\tau)$ fixed. We get by Lemma 2.1 (i) and (F3) that

$$\begin{aligned} \mathrm{ord}_q\, g(\tau) &= 6Nn\mathbf{B}_2(1/N) + 12Nn\mathbf{B}_2(0) \\ &= \mathrm{ord}_q\, g(\tau)^{\gamma} \\ &= \mathrm{ord}_q\, g_{\left[\begin{smallmatrix}a/N\\b/N\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}c/N\\d/N\end{smallmatrix}\right]}(\tau)^{24Nn} \\ &= 6Nn\mathbf{B}_2(\langle a/N\rangle) + 12Nn\mathbf{B}_2(\langle c/N\rangle). \end{aligned}$$

By considering the shape of the graph $y = \mathbf{B}_2(x)$ on the domain $[0,1)$, we deduce that

$$\langle c/N\rangle = 0 \quad \text{and} \quad \langle a/N\rangle = 1/N \text{ or } (N-1)/N,$$

and so $c \equiv 0 \pmod N$ and $a \equiv \pm 1 \pmod N$. Moreover, we achieve by the fact $\det(\gamma) = ad - bc = 1$ that $a \equiv d \equiv \pm 1 \pmod N$. On the other hand, we derive by (F3) and Lemma 2.1 (i) that

$$\begin{aligned} \mathrm{ord}_q\, g(\tau)^{\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]} &= \mathrm{ord}_q\, g_{\left[\begin{smallmatrix}0\\-1/N\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{24Nn} \\ &= 6Nn\mathbf{B}_2(0) + 12Nn\mathbf{B}_2(1/N) \\ &= \mathrm{ord}_q\, (g(\tau)^{\gamma})^{\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]} \\ &= \mathrm{ord}_q\, g(\tau)^{\left[\begin{smallmatrix}b&-a\\d&-c\end{smallmatrix}\right]} \\ &= \mathrm{ord}_q\, g_{\left[\begin{smallmatrix}b/N\\-a/N\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}d/N\\-c/N\end{smallmatrix}\right]}(\tau)^{24Nn} \\ &= 6Nn\mathbf{B}_2(\langle b/N\rangle) + 12Nn\mathbf{B}_2(\langle d/N\rangle), \end{aligned}$$

from which we conclude $b \equiv 0 \pmod N$. Hence γ belongs to $\pm\Gamma(N)$, which proves that $g(\tau)$ generates the field $\mathbb{C}(X(N))$ over $\mathbb{C}(X(1))$.

(ii) Let

$$F = \mathbb{Q}\left(j(\tau),\, \zeta_N g_{\left[\begin{smallmatrix}1/N\\0\end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau)^{24Nn}\right).$$

Then, F is a subfield of $\mathcal{F}_N$ and $\mathrm{Gal}(\mathcal{F}_N/F)$ is a subgroup of G_N. Let $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ be an element of G_N which leaves $\zeta_N g(\tau)$ fixed. Letting $\beta = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$, we deduce by Lemma 2.1 (i), (F3) and (A1) that

$$\begin{aligned}
\mathrm{ord}_q\ (\zeta_N g(\tau))^\beta &= \mathrm{ord}_q\ \zeta_N g_{\left[\begin{smallmatrix} 0 \\ -1/N \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{24Nn} \\
&= 6Nn\mathbf{B}_2(0) + 12Nn\mathbf{B}_2(1/N) \\
&= \mathrm{ord}_q\ ((\zeta_N g(\tau))^\alpha)^\beta \\
&= \mathrm{ord}_q\ (\zeta_N^d g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} 0 \\ d/N \end{smallmatrix}\right]}(\tau)^{24Nn})^\beta \\
&= \mathrm{ord}_q\ \zeta_N^d g_{\left[\begin{smallmatrix} 0 \\ -1/N \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} d/N \\ 0 \end{smallmatrix}\right]}(\tau)^{24Nn} \\
&= 6Nn\mathbf{B}_2(0) + 12Nn\mathbf{B}_2(\langle d/N \rangle).
\end{aligned}$$

Thus we obtain $d \equiv \pm 1 \pmod N$. It is clear that if $N = 2$, then $d \equiv 1 \pmod N$. If $N \geq 3$ and $d \equiv -1 \pmod N$, then we get by (A1), (F2) and (F3) that

$$\zeta_N g(\tau) = \zeta_N g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{24Nn} = (\zeta_N g(\tau))^\alpha = \zeta_N^{-1} g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{24Nn},$$

and so $\zeta_N^2 = 1$. But, this is impossible. Therefore, we always have $d \equiv 1 \pmod N$, from which $F = \mathcal{F}_N$ by Galois theory.

□

Remark 4.5. It is well known that $g_{\mathbf{v}}(\tau)^{12N}$ are integral over $\mathbb{Z}[j(\tau)]$ for all $\mathbf{v} \in \mathcal{V}_N$ ([6, §3]). Thus, if $n > 0$ and $g(\tau) = g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{24Nn}$, then there is a polynomial $f_N(x, y) \in \mathbb{Z}[x, y]$ for which $f_N(x, y)$ is monic in x and $f_N(g(\tau), j(\tau)) = 0$. That is, the equation $f_N(x, y) = 0$ gives rise to an affine singular model of the modular curve $X(N)$ over $\mathbb{Q}$. For example, if $N = 2$ and $n = 1$, then one can estimate

$$\begin{aligned}
f_N(x, y) = {} & x^6 + (-2y^3 + 2^8 \cdot 3^2 y^2 + 2^{18} \cdot 3y - 2^{25} \cdot 3)x^5 \\
& + (y^6 - 2^9 \cdot 3^2 y^5 + 2^{16} \cdot 3^2 \cdot 13y^4 - 2^{25} \cdot 163y^3 + 2^{36} \cdot 3^3 y^2 - 2^{44} \cdot 3y + 2^{48} \cdot 3 \cdot 5)x^4 \\
& + (-2^{25} y^6 + 2^{40} \cdot 3 \cdot 67y^4 - 2^{55} \cdot 7y^3 + 2^{57} \cdot 3^2 \cdot 47y^2 + 2^{67} \cdot 3^2 y - 2^{74} \cdot 5)x^3 \\
& + (2^{48} y^6 - 2^{57} \cdot 3^2 y^5 + 2^{64} \cdot 3^2 \cdot 13y^4 - 2^{73} \cdot 163y^3 + 2^{84} \cdot 3^3 y^2 - 2^{92} \cdot 3y + 2^{96} \cdot 3 \cdot 5)x^2 \\
& + (-2^{97} y^3 + 2^{104} \cdot 3^2 y^2 + 2^{114} \cdot 3y - 2^{121} \cdot 3)x + 2^{144}
\end{aligned}$$

by using the Fourier expansions of Siegel functions and $j(\tau)$ (see [4, p. 29] and [1, Theorem 12.17]).

5 Application to class fields

Let K be an imaginary quadratic field and $N \geq 2$. As a consequence of the main theorem of complex multiplication, we obtain that $H_K = K(j(\tau_K))$ and

$$K_{(N)} = K(h(\tau_K) \mid h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K) \tag{19}$$

([10, Theorem 1 and Corollary to Theorem 2 in Chapter 10]). Let

$$\min(\tau_K, \mathbb{Q}) = x^2 + B_K x + C_K \in \mathbb{Z}[x],$$

and define a subgroup $W_{K,N}$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by

$$W_{K,N} = \left\{ \gamma = \begin{bmatrix} t - B_K s & -C_K s \\ s & t \end{bmatrix} \mid t,\, s \in \mathbb{Z}/N\mathbb{Z} \text{ such that } \gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

If K is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, then by the Shimura reciprocity law we have the isomorphism

$$\begin{array}{rcl} W_{K,N}/\{\pm I_2\} & \xrightarrow{\sim} & \mathrm{Gal}(K_{(N)}/H_K) \\ \gamma & \mapsto & (h(\tau_K) \mapsto h^{\gamma}(\tau_K) \mid h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K) \end{array} \tag{20}$$

([13, §3]).

Lemma 5.1. *If m is a positive integer such that $\zeta_m \in K_{(N)}$, then m divides $12N$.*

Proof. See [4, Lemma 4.3 (i) in Chapter 9]. □

Let $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v} \in \mathcal{V}_N}$ be a totally primitive Fricke family of level N, and let $d_N(\tau)$ be the discriminant of $h_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{12N}$ over $\mathcal{F}_1$. Define an equivalence relation $\sim$ on the set $\mathcal{V}_N$ by

$$\mathbf{u} \sim \mathbf{v} \iff \mathbf{u} \equiv \pm \mathbf{v} \pmod{\mathbb{Z}^2}.$$

Since $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ and $\{h_{\mathbf{v}}(\tau)^{12N}\}_{\mathbf{v} \in \mathcal{V}_N}$ is primitive, we get by (F3) that

$$d_N(\tau) = \pm \prod_{\substack{[\mathbf{u}],\,[\mathbf{v}] \in \mathcal{V}_N/\sim \\ \text{such that } [\mathbf{u}] \neq [\mathbf{v}]}} \left(h_{\mathbf{u}}(\tau)^{12N} - h_{\mathbf{v}}(\tau)^{12N} \right),$$

where $[\mathbf{u}]$ and $[\mathbf{v}]$ stand for the equivalences classes of $\mathbf{u}$ and $\mathbf{v}$ in $\mathcal{V}_N$, respectively. Note that $d_N(\tau)$ is a nonzero element of $\mathcal{F}_1$ which is weakly holomorphic. Thus it has only finitely many zeros on the modular curve $X(1)$, and hence the set

$$S_N = \{\text{imaginary quadratic fields } K \mid d_N(\tau_K) = 0\} \cup \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$$

is finite.

THEOREM 5.2. *Let K be an imaginary quadratic field lying outside the set S_N, and let $\{h_{\mathbf{v}}(\tau)\}_{\mathbf{v}\in\mathcal{V}_N}$ be a totally primitive Fricke family of level N. If $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)$ is nonzero, then*

$$h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n$$

generates $K_{(N)}$ over H_K for any nonzero integer n.

PROOF. Suppose on the contrary that $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n$ does not generates $K_{(N)}$ over H_K for some nonzero integer n. Then, there is a nonidentity element α of $\mathrm{Gal}(K_{(N)}/H_K)$ leaving $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n$ fixed. Due to the isomorphism given in (20), the Galois element α corresponds to a matrix $\begin{bmatrix} t-B_Ks & -C_Ks \\ s & t \end{bmatrix}$ in $W_{K,N}/\{\pm I_2\}$ with $\begin{bmatrix} s \\ t \end{bmatrix} \neq \pm \begin{bmatrix} 0 \\ 1 \end{bmatrix} \pmod N$. We then achieve that

$$\begin{aligned} h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n &= (h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n)^\alpha \\ &= (h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^\alpha)^n \\ &= h_{\left[\begin{smallmatrix}t-B_Ks & s\\ -C_Ks & t\end{smallmatrix}\right]\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n \quad \text{by the isomorphism in (20) and (F3)} \\ &= h_{\left[\begin{smallmatrix}s/N\\t/N\end{smallmatrix}\right]}(\tau_K)^n, \end{aligned}$$

from which we get

$$h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K) = \zeta h_{\left[\begin{smallmatrix}s/N\\t/N\end{smallmatrix}\right]}(\tau_K) \quad \text{for some } |n|\text{th root of unity.} \tag{21}$$

Since $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)$ and $h_{\left[\begin{smallmatrix}s/N\\t/N\end{smallmatrix}\right]}(\tau_K)$ belong to $K_{(N)}$ by (19), we deduce by Lemma 5.1 that ζ is a $12N$th root of unity. Thus we obtain by (21) that

$$h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^{12N} = h_{\left[\begin{smallmatrix}s/N\\t/N\end{smallmatrix}\right]}(\tau_K)^{12N},$$

which implies $d_N(\tau_K) = 0$. But, this contradicts that K does not belong to S_N.

Therefore, we conclude that if $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)$ is nonzero, then $h_{\left[\begin{smallmatrix}0\\1/N\end{smallmatrix}\right]}(\tau_K)^n$ generates $K_{(N)}$ over H_K for any nonzero integer n. □

REMARK 5.3. Let K be an imaginary quadratic field of discriminant d_K, and let n be a nonzero integer.

(i) Every weakly holomorphic function in $\mathcal{F}_1$ is a polynomial in $j(\tau)$ over $\mathbb{Q}$ ([10, Theorem 2 in Chapter 5]). Moreover, since $\mathrm{ord}_q\ j(\tau) = -1$ ([10, p. 45]), we see that $d_N(\tau)$ is a polynomial in $j(\tau)$ over $\mathbb{Q}$ of degree $|\mathrm{ord}_q\ d_N(\tau)|$. It is well known that $j(\tau_K)$ generates H_K over K (as we mentioned), and $[H_K : K] \to \infty$ as $|d_K| \to \infty$ ([1, p. 149]). Hence, if $|d_K|$ (≥ 7) is large enough so as to have $[H_K : K] > |\mathrm{ord}_q\ d_N(\tau)|$, then K does not belong to the set S_N.

(ii) Let $g(\tau) = g_{\left[\begin{smallmatrix} 1/N \\ 0 \end{smallmatrix}\right]}(\tau)^{12Nn} g_{\left[\begin{smallmatrix} 0 \\ 1/N \end{smallmatrix}\right]}(\tau)^{24Nn}$ be the function stated in Theorem 4.4. By making use of the Kronecker second limit formula one can also show that if $\gcd(N, 3 \cdot 5 \cdot 7 \cdot 13 \cdot d_K(d_K - 1)) = 1$, then $g(\tau_K)$ generates $K_{(N)}$ over the ground field K instead of H_K (see [8]).

References

[1] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.

[2] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, New York, 2005.

[3] I. S. Eum and D. H. Shin, *Determination of the Fricke families*, to appear in J. Korean Math. Soc.

[4] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.

[5] J. K. Koo, G. Robert, D. H. Shin and D. S. Yoon, *On Siegel invariants of certain CM-fields*, submitted, http://arxiv.org/abs/1508.05602.

[6] J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit. 264 (2010), no. 1, 137–177.

[7] J. K. Koo, D. H. Shin and D. S. Yoon, *Generators of Siegel modular function field of higher genus and level*, submitted, http://arxiv.org/abs/1604.01514.

[8] J. K. Koo and D. S. Yoon, *Construction of ray class fields by smaller generators and applications*, to appear in P. Roy. Soc. Edinb. A.

[9] J. K. Koo and D. S. Yoon, *Generators of the ring of weakly holomorphic modular functions for $\Gamma_1(N)$*, to appear in Ramanujan J.

[10] S. Lang, *Elliptic Functions*, 2nd edn, Grad. Texts in Math. 112, Spinger-Verlag, New York, 1987.

[11] R. Miranda, *Algebraic Curves and Riemann Surfaces*, Grad. Studies in Math., vol. 5, Amer. Math. Soc., 1995.

[12] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.

[13] P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory-its centenary and prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.

Applied Algebra and Optimization Research Center
Sungkyunkwan University
Suwon-si, Gyeonggi-do 16419
Republic of Korea

E-mail address: hoyunjung@skku.edu

Department of Mathematics
Hankuk University of Foreign Studies
Yongin-si, Gyeonggi-do 17035
Republic of Korea

E-mail address: dhshin@hufs.ac.kr

Department of Mathematical Sciences
KAIST
Daejeon 34141
Republic of Korea

E-mail address: jkkoo@math.kaist.ac.kr